Endfassung

GLOBALTRUST®
Certificate Practice Statement
[GCPS - ZDA Betriebsleitlinien]

Autor: Hans G. Zeger

Version 1.0a / 1. Februar 2015 -
OID-Nummer: 1.2.40.0.36.1.2.3.1
Gültigkeitshistorie OID-Nummer: 1.2.40.0.36.1.2.3.99

Redaktioneller Hinweis: Das vorliegende Dokument ist mit einer fortgeschrittenen Signatur versehen. Das Datum der Signatur kann aus verschiedenen rechtlichen und organisatorischen Gründen vom Datum des Gültigkeitsbeginns des Dokuments abweichen. Die Signatur gibt keine Auskunft über den Gültigkeitsbeginn des Dokuments, sondern bestätigt nur die Unversehrtheit des Inhalts.

INHALT

ANHANG

1. EINLEITUNG / INTRODUCTION

Dieses GLOBALTRUST® Certificate Practice Statement ergänzt die GLOBALTRUST® Certificate Policy (OID-Nummer: 1.2.40.0.36.1.1.8.1) und regelt die detaillierte Vorgangsweise für folgende Produktgruppen: GLOBALTRUST® und A-CERT.

Die sicherheitstechnischen Anforderungen und Maßnahmen des ZDA sind im Dokument GLOBALTRUST® Certificate Security Policy (OID-Nummer: 1.2.40.0.36.1.2.2.1) enthalten. Dieses Dokument ist nicht öffentlich verfügbar.

Produktgruppe GLOBALTRUST®

Die Zertifizierungsangebote des ZDA werden unter der Produktbezeichnung GLOBALTRUST® betrieben. Produkte die den Anforderungen der qualifizierten Signatur bzw. qualifizierten Zertifikaten entsprechen, können den Zusatz "QUALIFIED" erhalten, Produkte die den Anforderungen der fortgeschrittenen Signatur gemäß Signaturgesetz [SigG] entsprechen, können den Zusatz "ADVANCED" erhalten. Der Umfang der Gültigkeit ergibt sich aus der jeweils anzuwendenen Certificate Policy.

Produktgruppe A-CERT

Für die Produkte A-CERT ist der Herausgeber nicht Zertifizierungsdienstanbieter (ZDA) sondern Betreiber. Der Betrieb erfolgt nach denselben Standards wie für GLOBALTRUST® gemäß den Policies zu den jeweiligen Produkten. Für die Produkte A-CERT ist der in Österreich nach dem Verreinsrecht eingetragene Verein "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (ZVR 774004629), in Folge kurz "Verein" ZDA.

Produktdokumentation

Die Liste der gemäß der GLOBALTRUST® Certificate Policy, des GLOBALTRUST® Certificate Practice Statement und GLOBALTRUST® Certificate Security Policy angebotenen Zertifizierungsprodukte zu GLOBALTRUST® und A-CERT, eine Beschreibung und der Verweis auf ihre jeweils gültigen Dokumente wird auf der Website des Betreibers veröffentlicht und laufend aktualisiert.

Diese Produktinformation dient zur Unterstützung in der Auswahl und Anwendung der richtigen Zertifizierungsprodukte und ersetzt nicht den verbindlichen Verweis auf die anzuwendende Certificate Policy, die in jedem ausgelieferten Zertifikat enthalten ist.

Ergänzende Bestimmungen für mobile Signaturdienste

Mobile Signaturdienste können den Zusatz "MOBILE" enthalten oder sind auf andere Weise eindeutig als mobiler Signaturdienst gekennzeichnet. Die Bezeichnung kann alleine oder in Verbindung mit "QUALIFIED" verwendet werden.

Mobile Signaturdienste können als qualifizierte, fortgeschrittene oder einfache elektronische Signaturdienste angeboten werden.

Mobile Signaturdienste werden mittels Mobiltelefonen oder anderer geeigneter mobiler technischer Einheiten ausgelöst. Mobile Signaturdienste werden als Serverdienste oder als

"direkte elektronische Signatur" (Signatur am Endgerät) in der mobilen technischen Einheit angeboten.

Bei Serverdiensten entspricht die technische Einrichtung denselben Sicherheitsanforderungen wie sie der Ausstellung von Zertifikaten unterliegt (⇨ GLOBALTRUST® Certificate Security Policy).

Die mobile technische Einheit übernimmt bei Serverdiensten die Rolle des sicherheitsverstärkenden Faktors um neben dem Wissen um ein Geheimnis (z.B. Wissen der Signatur-PIN zum Auslösen der Signaturfunktion) auch den Besitz der alleinigen signaturauslösenden Komponente (z.B. Mobiltelefons) sicherzustellen. Dies entspricht der Zwei-Faktor-Authentifizierung gegenüber dem serverseitigen Signaturerstellungsgerät und ist analog dem Vorgehen bei chipkarten-basierten Signaturlösungen (Besitz der Chipkarte und Wissen des PIN zum Auslösen der Signaturfunktion). Der Besitz der mobilen technischen Einheit wird insbesondere durch Abfrage eines Einmalpasswortes, dass über geeignete Übertragungswege übermittelt wurde (z.B. Verifikations-SMS) überprüft.

An ein Mobiltelefon werden bei einer serverbasierten Signatur keine besonderen Anforderungen gestellt. Als mobile technische Einheiten für Serverlösungen kommen alle Systeme in Betracht, die manipulationssicher eindeutig identifiziert und einer Person zugeordnet werden können. Geeignete technische Einheiten werden auf der Website des ZDA gelistet und laufend ergänzt.

Als mobile technische Einheiten für die qualifizierte elektronische Signatur sind jene Komponenten geeignet, die eine Zertifizierung nach CC EAL4+ oder FIPS 140-2 L2 aufweisen, insbesondere können das SIM-Karten mit kryptographischen Coprozessor, microSD-Karten oder USB-Token sein.

Spezifische Verpflichtungen des ZDA bei der Erbringung von Mobilen Signaturdiensten

Im Rahmen der Erbringung der elektronischen Signatur als Serverdienst verpflichtet sich der ZDA serverseitig zur Einhaltung derselben GLOBALTRUST® Certificate Security Policy wie bei der Erbringung anderer Zertifizierungsdienste, insbesondere der qualifizierten Zeitstempeldienste.

Im Rahmen der direkten elektronischen Signatur wird sicher gestellt, dass diese nur auf Geräten erfolgen kann, die den technischen Anforderungen entsprechen. Im Falle der qualifizierten elektronischen Signatur muss die dafür vorgesehene Signaturkomponente die Zertifizierung einer Bestätigungsstelle aufweisen.

Serverbasierte Signaturdienste werden gemäß derselben ⇨ betrieben, wie die sonstigen Zertifizierungsdienste des Betreibers.

Der Betreiber behält sich vor, zu den serverbasierten Signaturdiensten auf Basis der GLOBALTRUST® Certificate Policy und der GLOBALTRUST® Certificate Security Policy ein ergänzendes Practice Statement zu veröffentlichen.

1.1 Übersicht / Overview

Dokumente werden in eckigen Klammern [] zitiert und finden sich im ⇨ Anhang A:1 Bibliographie (p58) mit den bibliographischen Angaben gelistet. Sie werden mit Stand 1.

Februar 2015 zitiert, aber in der jeweils gültigen Fassung bzw. zutreffenden Folgestandards angewandt.

Die Gültigkeit von Weblinks bezieht sich, sofern nicht ausdrücklich anders vermerkt auf den Redaktionsschluss dieses Dokuments.

Das vorliegende Dokument "GLOBALTRUST® Certificate Practice Statement" (GCPS) beschreibt alle wesentlichen betrieblichen Abläufe zur Verwaltung und Ausstellung von Signaturerstellungseinheiten, Signaturerstellungsdaten und Zertifikate.

Anpassungen der Anhänge, insbesondere um aktuelle technische Entwicklungen zu berücksichtigen, bedeuten keine Änderung der betrieblichen Abläufe, insbesondere keine Änderung des Sicherheitskonzepts, wenn sie in Übereinstimmung mit dem vorliegenden Dokument und der "GLOBALTRUST® Certificate Security Policy" erfolgen.

Die GLOBALTRUST® Certificate Policy beschreibt die generellen betrieblichen und technischen Anforderungen zu den ausgegebenen Zertifikaten, soweit diese nicht im vorliegenden GLOBALTRUST® Certificate Practice Statement (GCPS) detailliert behandelt sind. Die GLOBALTRUST® Certificate Policy ist mit OID-Nummer und Abrufstandort in jedem ausgegebenen Zertifikat eingetragen.

1.2 Dokumenttitel und -identifikation / Document name and identification

Dokumententitel: "GLOBALTRUST® Certificate Practice Statement" (GCPS)

Dieses Practice Statement hat die OID-Nummer: 1.2.40.0.36.1.2.3.1).

Das vorliegende Dokument tritt mit dem Tag der Veröffentlichung auf der Website des Betreibers in Kraft. Sofern nicht anders vermerkt endet die Gültigkeit der früheren Version des Dokuments mit Beginn der Gültigkeit der neuen Version.

Das vorliegende Dokument wurde konform zu [RFC3647] erstellt.

Das vorliegende Dokument beschreibt alle betrieblichen Abläufe des ZDA in konzeptioneller Form und ist über die Website des Betreibers öffentlich abrufbar.

1. V1.0 STAMMFASSUNG

Redaktionsschluss: 1. Februar 2015

1.3 Beteiligte / PKI participants

Gemäß GLOBALTRUST® Certificate Policy

1.3.1 Zertifizierungsdienstanbieter / Certification authorities

Gemäß GLOBALTRUST® Certificate Policy

1.3.2 Registrierungsstelle / Registration authorities

Gemäß GLOBALTRUST® Certificate Policy

1.3.3 Signator / Subscribers

Gemäß GLOBALTRUST® Certificate Policy

1.3.4 Nutzer / Relying parties

Gemäß GLOBALTRUST® Certificate Policy

1.3.5 Weitere Beteiligte / Other participants

Gemäß GLOBALTRUST® Certificate Policy

1.4 Verwendungszweck der Zertifikate / Certificate usage

Gemäß GLOBALTRUST® Certificate Policy

1.4.1 Verwendungszweck / Appropriate certificate uses

Gemäß GLOBALTRUST® Certificate Policy

1.4.2 Untersagte Nutzung der Zertifikate / Prohibited certificate uses

Gemäß GLOBALTRUST® Certificate Policy

1.5 Policy Verwaltung / Policy administration

Gemäß GLOBALTRUST® Certificate Policy

1.5.1 Zuständigkeit für das Dokument / Organization administering the document

Das vorliegende Dokument unterliegt der alleinigen Verantwortung des ZDA.

1.5.2 Kontaktperson / Contact person

Anfragen zum Dokument sind an den Betreiber zu richten. Die aktuellen Kontaktdaten sind auf der Website des Betreibers gelistet.

1.5.3 Person die die Eignung der CPS bestätigt / Person determining CPS suitability for the policy

Gemäß GLOBALTRUST® Certificate Policy

1.5.4 Verfahren zur Freigabe der CPS / CPS approval procedures

Gemäß GLOBALTRUST® Certificate Policy

1.6 Definitionen und Kurzbezeichnungen / Definitions and acronyms

Gemäß GLOBALTRUST® Certificate Policy

Zusätzlich gelten folgende Definitionen:

Produktzusatz ADVANCED
Bezeichnet Zertifikate, die für die Erstellung fortgeschrittener elektronischer Signaturen geeignet sind.

Produktzusatz GOVERNMENT
Bezeichnet Zertifikate, die für die Erstellung von Amtssignaturen nach dem österreichischen E-Government-Gesetz geeignet sind. Diese Zertifikate sind gleichzeitig für fortgeschrittene elektronische Signaturen geeignet.

Produktzusatz COMPANY
Beschreibt alle Produkte, bei denen Sub-Zertifikate für Signatoren ausgestellt werden. Die Regeln zur Vergabe der Sub-Zertifikate können durch zusätzliche COMPANY-Policies spezifiziert werden. Diese sind im ausgegebenen Sub-Zertifikat eingetragen.

Produktzusatz QUALIFIED
Bezeichnet qualifizierte Zertifikate, die für die Erstellung fortgeschrittener und qualifizierter Signaturen geeignet sind. Diese Zertifikate unterliegen zusätzlichen Anwendungsbeschränkungen.

Produktzusatz CLIENT, SERVERCERT, FREECERT, DEMO
Bezeichnet Zertifikate, die für die Erstellung sonstiger Signaturen (einfache Signaturen) und zur Verschlüsselung geeignet sind. Sonstige nicht angeführte Zusätze bezeichnen immer Zertifikate, die ausschließlich zur Erstellung einfacher Signaturen und zur Verschlüsselung geeignet sind.

Testzertifikate
Bezeichnet Zertifikate, die auf Basis des X.509v3-Standards zu Testzwecken ausgestellt werden. Eine Identitätsprüfung der Antragsteller (Signatoren) findet nicht statt. Testzertifikate sind erkennbar, wenn zumindest eine der Bedingungen erfüllt ist:
- bei X509v3-Zertifikaten lautet die CN-Bezeichnung des ZDAs (Issuer) GLOBALTRUST FREECERT, GLOBALTRUST ADVANCED TEST, GLOBALTRUST GOVERNMENT TEST, allgemein GLOBALTRUST ***[1] TEST
- bei X509v3-Zertifikaten hat die O-Bezeichnung (Organisationsbezeichnung) des Antragstellers (Subject) den führenden Vermerk "Test: ", bei Privatpersonen den Eintrag "Testzertifikat",
- bei X509v3-Zertifikaten enthält das Zertifikat eine entsprechende Erweiterung (siehe CPS 7.1.2)
- bei anderen Zertifikatstypen sind ZDA- und/oder Antragstellerangaben so zu wählen, das ihre Testeigenschaft eindeutig zum Ausdruck kommt.

Qualifizierte Zertifikate können nicht in Form von Testzertifikaten ausgestellt werden.

[1] *** = beliebiger zulässiger Produktzusatz

2. VERÖFFENTLICHUNG UND AUFBEWAHRUNG / PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Aufbewahrung / Repositories

Die aktuelle Version dieses Dokuments ist über die Website des Betreibers abrufbar.

Historische Versionen des Dokuments sind bei der Aufsichtsstelle abzurufen oder unter der OID-Nummer 1.2.40.0.36.1.2.3.99 auf der Website des Betreibers abgelegt. Eine englische Übersetzung dieses Practice Statements wird unter der OID-Nummer 1.2.40.0.36.1.2.3.12 veröffentlicht[2].

Über die Website bzw. sofern von den Zertifikatsinhabern verfügbar per E-Mail wird zeitgerecht über Änderungen informiert, die im GLOBALTRUST® Certificate Practice Statement vorgenommen werden.

2.2 Veröffentlichung von Zertifizierungsinformationen / Publication of certification information

Gemäß GLOBALTRUST® Certificate Policy

2.3 Häufigkeit der Veröffentlichung / Time or frequency of publication

Gemäß GLOBALTRUST® Certificate Policy

2.4 Zugangsbeschränkungen / Access controls on repositories

Gemäß GLOBALTRUST® Certificate Policy

[2] Die Veröffentlichung erfolgt nach Abschluss der Genehmigung des GLOBALTRUST® Certificate Practice Statement durch die Aufsichtsbehörde und hat informativen Charakter.

3. IDENTIFIZIERUNG UND AUTHENTIFIKATION / IDENTIFICATION AND AUTHENTICATION

3.1 Benennung / Naming

Die eindeutige Zuordnung des Zertifikats zum Signator ist sicher gestellt durch:
- Erstellung des PKCS#10-Requests (bei X.509v3 Zertifikaten) als Grundlage für die Zertifizierung,
- Erzeugung des Zertifikats nach Überprüfung aller Antragsdaten auf ihre Korrektheit durch eine Registrierungsstelle oder an der Zertifizierungsstelle des ZDAs.

3.1.1 Arten der Benennung / Types of names

Gemäß GLOBALTRUST® Certificate Policy

3.1.2 Notwendigkeit für aussagekräftige Namen / Need for names to be meaningful

Gemäß GLOBALTRUST® Certificate Policy

3.1.3 Behandlung von Anonymität oder Pseudonymen von Antragstellern / Anonymity or pseudonymity of subscribers

Gemäß GLOBALTRUST® Certificate Policy

3.1.4 Interpretationsregeln für verschiedene Benennungsformen / Rules for interpreting various name forms

Gemäß GLOBALTRUST® Certificate Policy

3.1.5 Einmaligkeit von Benennungen / Uniqueness of names

Gemäß GLOBALTRUST® Certificate Policy

3.1.6 Anerkennung, Authentifikation und Rolle von Markennamen / Recognition, authentication, and role of trademarks

Gemäß GLOBALTRUST® Certificate Policy

3.2 Erstmalige Identitätsfeststellung / Initial identity validation

Gemäß GLOBALTRUST® Certificate Policy

3.2.1 Nachweis über den Besitzes des privaten Schlüssels / Method to prove possession of private key

Die Prüfung kann insbesondere durch die technische Prüfung von signierten Daten (Certificate Signing Request) unter Beachtung geeigneter Algorithmen nach [ETSI TS 102 176] passieren.

3.2.2 Authentifikation der Organisation / Authentication of organization identity

Gemäß GLOBALTRUST® Certificate Policy

3.2.3 Identitätsprüfung von Personen / Authentication of individual identity

Gemäß GLOBALTRUST® Certificate Policy

3.2.4 Nicht-verifizierte Antragstellerdaten / Non-verified subscriber information

Ergänzend zur GLOBALTRUST® Certificate Policy sind nicht-verifzierte Angaben unter folgenden Bedingungen zulässig:
- beim Zertifikat handelt es sich um ein als Testzertifikat gekennzeichnetes Zertifikat
- Nicht-verifizierte Antragstellerangaben erhalten in unmittelbarer Nähe die zusätzliche Bezeichnung "nicht-verifiziert", z.B. <Angaben> (nicht-verifiziert)

3.2.5 Nachweis der Vertretungsbefugnis / Validation of authority

Ergänzend zur GLOBALTRUST® Certificate Policy sind zusätzliche Angaben zur vertretenen Organisation erforderlich: Wird von einer Person ein Zertifikat beansprucht, mit dem Rechtsgeschäfte für eine Organisation oder eine andere Person erledigt werden können, dann sind folgende Zusatzinformationen obligatorisch: Name und Anschrift der Organisation/Person und Organisationsform (z.B. eingetragener Verein, protokolliertes Unternehmen, ...). Weiters ist zumindest eine Stelle anzugeben, die als Auskunftsstelle für diese Organisation geeignet ist (z.B. zugehörige Kammer, Firmenbuch, Vereinsbehörde, Aufsichtsbehörde, ...). Sind Organisationen per Gesetz eingerichtet, ist statt der Auskunftsstelle die Gesetzesstelle anzuführen, auf Grund der die Einrichtung erfolgte.

Weiters kann angegeben werden, für welche Aufgaben (Aufgabenbereiche) der Signator vertretungsbefugt ist (gegebenenfalls ist der Umfang wertmäßig oder vorgangsmäßig zu begrenzen).

3.2.6 Kriterien für Interoperabilität / Criteria for interoperation

Gemäß GLOBALTRUST® Certificate Policy

3.3 Identifikation und Authentifikation für Schlüsselerneuerung / Identification and authentication for re-key requests

Gemäß GLOBALTRUST® Certificate Policy

3.3.1 Identifikation und Authentifikation für routinemäßige Schlüsselerneuerung / Identification and authentication for routine re-key

Gemäß GLOBALTRUST® Certificate Policy

3.3.2 Identifikation und Authentifikation für Schlüsselerneuerung nach Widerrufen / Identification and authentication for re-key after revocation

Gemäß GLOBALTRUST® Certificate Policy

3.4 Identifikation und Authentifikation für Widerrufsanträge / Identification and authentication for revocation request

Gemäß GLOBALTRUST® Certificate Policy

4. ANFORDERUNGEN ZERTIFIKATSLEBENSZYKLUS / CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Antragstellung / Certificate Application

1. Anträge zur Zertifizierung werden sowohl online als auch offline entgegen genommen. Insbesondere können Anträge mittels Online-Formular, schriftlich, per eMail, per Fax, sonstige elektronische Kommunikationsmittel, telefonisch, persönlich, insbesondere auch mündlich gestellt werden. Über die Möglichkeiten der Antragstellung informiert die Website des ZDA, das GLOBALTRUST® Certificate Practice Statement oder sonstige öffentlich zugängliche Publikationen des ZDA.
2. Das Antragsformular und alle erforderlichen Informationen sind über die Website des ZDAs oder der Vertriebspartner zugänglich.
3. Der Zertifikatsantrag enthält folgende Mindestangaben:
   den Namen und die Anschrift des Signators.
4. Angaben zum Zweck der Verwendung des Zertifikats:
   Die Angaben zum Zweck können je nach bereitgestelltem Zertifizierungsdienst optional oder obligatorisch sein.
5. Anträge für Serverzertifkate enthalten zumindest einen Domainnamen oder eine IP-Adresse.
6. Kenntnisnahme und Zustimmung zu den Allgemeinen Betriebs- und Nutzungsbedingungen (AGB's) des ZDAs, zur vorliegenden Policy und gegebenenfalls zu weiteren zertifizierungsabhängigen Vereinbarungen.
7. Mit dem Antragsteller wird eine sichere Zugangsweise (etwa ein Aktivierungspasswort) vereinbart, mit dessen Hilfe er nach erfolgter Zertifizierung Zugang zu den bereitgestellten Unterlagen (persönliches Zertifikat, privater Schlüssel, ...) hat.

4.1.1 Berechtigung zur Antragstellung / Who can submit a certificate application

Der Identitätsnachweis gilt als erbracht, wenn Signaturerstellungsdaten und -unterlagen an dieselbe Adresse (in derselben Form) zugestellt werden können, die bei einer vormaligen Identitätsprüfung festgelegt wurden und zwischenzeitlich kein Widerruf erfolgte.

4.1.2 Anmeldungsverfahren und Verantwortlichkeiten / Enrollment process and responsibilities

Ergänzend zur GLOBALTRUST® Certificate Policy gilt:

Angaben des Signators zur Hardware auf der der private Schlüssel generiert wird, werden vom ZDA dahingehend geprüft, ob das angegebene Produkt tatsächlich zur gesicherten Verwahrung eines privaten Schlüssels geeignet ist. Grundlage dieser Überprüfung sind Herstellerangaben ("Selbst-Deklaration") oder Berichte von Bestätigungsstellen.
Ein X.509v3-Zertifikat erhält dann folgende Erweiterung:
1.2.40.0.36.4.1.2: <verwendete Hardware>

Unter "<verwendete Hardware>" wird die handelsübliche oder durch eine Bestätigungsstelle verwendete Bezeichnung zur eindeutigen Kennzeichnung der Hardware angegeben.

Bei qualifizierten Zertifikaten sind zusätzlich allfällig erforderliche Bestätigungen der Aufsichtsstellen einzuholen.

4.2 Bearbeitung von Zertifkatsanträgen / Certificate application processing

Ergänzend zur GLOBALTRUST® Certificate Policy gilt:

Es wird geprüft, ob die technischen Eigenschaften des Schlüssels des Signators den vom Zertifiaktstypen abhängigen Anforderungen entspricht.

Zur Prüfung der Angaben einer Organisation können qualifizierte behördliche Informationsquellen, insbesondere zusätzlich das amtliche Telefonbuch oder der Amtskalender herangezogen werden. Organisationen, deren Daten weder über eine geeignete qualifizierte behördliche Informationsquelle abrufbar noch per Gesetz eingerichtet sind, werden Privatpersonen gleichgestellt behandelt. Die Organisationsangaben werden als optionale Zusatzangaben, vergleichbar dem Beruf oder der Qualifikation einer Privatperson angesehen.

Muss vor der Eintragung in ein Zertifkat ein Domainname geprüft werden, so passiert dies mit einer der folgenden Methoden:
1. Beim Registrar verifizieren, dass Domaininhaber und Antragsteller ident sind.
2. Direkte Kommunikation mit dem Domaininhaber über eine Adresse, E-Mail Adresse oder Telephonnummer die entweder vom Registrar zur Verfügung gestellt wurde oder einem WHOIS Eintrag entnommen wurde.
3. Eine schriftliche Bestätigung des Domaininhabers, des Registrars oder einer in den WHOIS Daten angeführten Person.
4. Direkte Kommunikation mit dem Domaininhaber über eine generische E-Mail Adresse, beispielsweise admin@domainname oder webmaster@domainname. Dabei können Teile des Domainnamens weggelassen werden.
5. Der Antragsteller kann die Kontrolle über die Domain praktisch demonstrieren, insbesondere durch eine abgesproche Änderung einer Webseite
6. Eine andere passende und wohldokumentierte Methode, die selbe Sicherheit wie die obigen gewährleistet.

Bei EV Zertifikaten sind nur die Methoden 1-5 zulässig.

Muss vor der Eintragung in ein Zertifkat eine IP-Adresse geprüft werden, so passiert dies mit einer der folgenden Methoden:
1. Der Antragsteller kann die Kontrolle über die Domain praktisch demonstrieren, insbesondere durch eine abgesproche Änderung einer Webseite.
2. Durch Prüfung von Informationen von internationalen oder regionalen Registrierungs-Agenturen für IP-Adressen (etwa IANA oder RIPE).
3. Der Domainname, der von der IP-Adresse mittels reverse lookup ermittelt wurde, wurde entsprechend den Bestimmungen dieser Policy geprüft.

4. Eine andere passende und wohldokumentierte Methode, die selbe Sicherheit wie die obigen gewährleistet.

Zusätzliche Prüfungen werden ausdrücklich vorbehalten und können insbesondere erforderlich sein, wenn
- die Auskünfte der zuständigen Auskunftsstellen ungenügend sind,
- Zweifel an der Verfügungsberechtigung über bestimmte Nummern- oder Namenselemente bestehen (etwa Verfügungsberechtigung über einen bestimmten Domainnamen),
- die Vertretungsbefugnis nicht ausreichend umschrieben bzw. dokumentiert ist,
- bei sonstigen Widersprüchen oder Unklarheiten im Zertifizierungsantrag,
- ein Zertifikatsantrag als Hochrisikofall betrachtet wird (insbesondere wenn die Domain für die ein Serverzertifikat ausgestellt werden soll ein bekanntes Ziel von Phishingangriffen darstellt)
- es in der Vergangenheit Antragsablehnungen oder Widerrufe gab, die auf Hinweise auf betrügerische Handlungen zurückzuführen waren und die mit dem bestehenden Antrag in Zusammenhang stehen.

Die Vorgangsweisen in diesen Fällen sind intern dokumentiert.

Soll ein Domainname mit einer Wildcard eingetragen werden, so muss jedenfalls der gesamte durch diese Wildcard abgedeckte Domainbereich wie oben beschrieben geprüft werden. Der Einsatz von Wildecards bei EV-Zertifikaten ist nicht zulässig.

Ergänzende Prüfschritte bei Antrag eines EV-Zertifikates

Ergänzend zu den allgemeinen Prüfschritten bei Antragstellung werden in diesem Abschnitt die ergänzenden Prüfschritte bei der Antragstellung eines EV-Zertifikates zusammen gefasst.

EV Zertifikate werden nur für Domainnamen die sich ausschließlich aus Zeichen des lateinischen Alphabets und gebräuchlichen Trennzeichen (Bindestrich) zusammensetzen ausgestellt.

Anträge für EV Zertifikate müssen von einer oder mehreren hinreichend autorisierten Person(en) die von der antragstellenden Organisation namhaft gemacht werden, geprüft, genehmigt und der Vertrag rechtlich bindend bestätigt werden. Die Unterschriften des Zertifikatsantrages und des Subscriber Agreements werden so geprüft, dass es hinreichend plausibel ist, dass sie von den richtigen Personen stammen. Von den beteiligten Personen wird jedenfalls Name, Titel, Verhältnis zur antragstellenden Organisation und die entsprechende Vertretungsvollmacht geprüft.

Außerdem gilt:
- EV Zertifikate werden nur an private, öffentliche oder internationale Organisationen (⇨ 3.2.5 Nachweis der Vertretungsbefugnis / Validation of authority, p19) ausgestellt
- Es werden keine EV Zertifikate an Organisationen ausgestellt, mit denen dem ZDA aufgrund von lokalen gesetzlichen Bestimmungen Handelsbeziehungen untersagt sind, sei es unmittelbar oder mittelbar aufgund des Herkunftslandes der Organisation- Bei einer privaten Organisation wird bei der angegebenen Auskunftsstelle (⇨ 3.2.5 Nachweis der Vertretungsbefugnis / Validation of authority, p19) überprüft, ob die Registirierung der antragstellenden Organisation nicht als abgelaufen, ungültig oder veraltet gekennzeichnet ist

- Bei privaten Organisationen wird geprüft, ob eine tatsächliche physische Representanz besteht
- Bei internationalen Organisationen, die aufgrund eines Vertrages, Abkommen oder einer Konvention zwischen mehreren souveränen Staaten eingerichtet wurden, wird die Existenz entweder über das konstituierende Dokument oder durch die Bestätigung einer Behörde eines Signatarstaates oder durch Kontrolle der vom CA/Browser Forum insbesondere auf http://www.cabforum.org veröffentlichten Liste geprüft.
- Bei privaten Organisationen die formelle Existenz und Identität, etwaige Pseudonyme, offizieller Name und Registrierung, Name einer vertretungsbevollmächtigten Person und falls notwendig, Relationen zu Mutter-, Tochter- oder Schwesterunternehmen.
  Bei gesetzlich eingerichteten und internationalen Organisationen die formelle Existenz, der Name und die Registrierungsnummer (falls vorhanden).
  Es wird geprüft, ob es sich bei der angegebenen Adresse um einen tatsächlichen Geschäftsstandort (und nicht nur einen Briefkasten) der antragstellenden Organisation oder eines Mutter-/Tochterunternehmens handelt.
  Die Telefonnummer des Geschäftsstandortes wird geprüft. Dazu wird jedenfalls die Nummer durch einen Anruf verifiziert. Als Quelle der Telefonnummer wird entweder auf die Auskunft des Telefonbetreibers oder einer passenden Auskunftstelle ('qualifizierte unabhängige Informationsquelle', QIIS oder eine 'qualifizierte behördliche Infromationsquelle', QGIS) oder ein geprüftes 'Rechtgutachten' oder die 'Bestätigung eines Wirtschaftsprüfers' vertraut.

Die Prüfung gilt als erfolgreich wenn:
1. die Auskunftsstelle, die zur Prüfung der Existenz der Organisation herangezogen wurde, eine 'qualifizierte behördliche Informationsquelle' (QGIS) ist und die dort angegebene Adresse der des Antrages entspricht oder
2. ein geprüftes 'Rechtsgutachten' oder eine geprüfte 'Bestätigung eines Wirtschaftsprüfers' vorliegt oder
3. durch Vorort-Prüfung einer autorisierten Person.

Sofern sich der Geschäftsstandort nicht im selben Staat wie der Ort der Registrierung befindet ist nur der oben angebene Punkt 2. zulässig.

Sofern die geprüfte Registrierung der Organisation jünger als drei Jahre ist, wird die operative Existenz der Organisation geprüft. Dazu wird entweder auf eine Auskunft des Bankinstitutes der Organisation über das Vorhandensein eines aktiven Kontos zurückgegriffen, auf ein geprüftes 'Rechtsgutachten' oder Bestätigung eines Wirtschaftsprüfers.

Sämtliche für die Ausstellung eines EV-Zertifikates notwendigen Informationen werden vor dessen Ausstellung von einer autorisierten Person geprüft, die nicht deren Sammlung durchgeführt hat. Etwaige Diskrepanzen sowie fehlerhafte oder fehlende Informationen werden vor der Ausstellung des Zertifikates dokumentiert und behoben, sofern dies nicht in einem akzeptablen Zeitrahmen möglich ist, wird der Zertifizierungsantrag abgelehnt.
Sofern Unterlagen nicht in der Arbeitssprache des Betreibers vorliegen, erfolgt die Prüfung durch eine Person mit den notwendigen sprachlichen Qualifikationen oder es wird auf die Dienste eines Übersetzers zurückgegriffen.

4.2.1 Durchführung Identifikation und Authentifikation / Performing identification and authentication functions

Gemäß GLOBALTRUST® Certificate Policy

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen / Approval or rejection of certificate applications

Gemäß GLOBALTRUST® Certificate Policy

4.2.3 Fristen für die Bearbeitung von Zertifkatsanträgen / Time to process certificate applications

Gemäß GLOBALTRUST® Certificate Policy

4.3 Zertifikatsausstellung / Certificate issuance

Gemäß GLOBALTRUST® Certificate Policy

4.3.1 Vorgehen des ZDA bei der Ausstellung von Zertifikaten / CA actions during certificate issuance

Gemäß GLOBALTRUST® Certificate Policy

4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate

Gemäß GLOBALTRUST® Certificate Policy

4.4 Zertifikatsannahme / Certificate acceptance

Gemäß GLOBALTRUST® Certificate Policy

4.4.1 Verfahren zur Zertifikatsannahme / Conduct constituting certificate acceptance

Gemäß GLOBALTRUST® Certificate Policy

4.4.2 Veröffentlichung der Zertifikate / Publication of the certificate by the CA

Gemäß GLOBALTRUST® Certificate Policy

4.4.3 Benachrichtigung von Dritten über die Zertifikatsaustellung / Notification of certificate issuance by the CA to other entities

Gemäß GLOBALTRUST® Certificate Policy

4.5 Schlüsselpaar und Zertifikatsnutzung / Key pair and certificate usage

4.5.1 Nutzung des privaten Schlüssels und des Zertifikates durch den Signator / Subscriber private key and certificate usage

Gemäß GLOBALTRUST® Certificate Policy

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikates durch Nutzer / Relying party public key and certificate usage

Gemäß GLOBALTRUST® Certificate Policy

4.6 Neuaustellung Zertifikat / Certificate renewal

Im Fall von qualifizierten Zertifikaten ist die Neuausstellung nicht zulässig.

4.6.1 Umstände für Neuaustellung eines Zertifikats / Circumstance for certificate renewal

Gemäß GLOBALTRUST® Certificate Policy

Im Fall von qualifizierten Zertifikaten ist die Neuausstellung ohne Erzeugung eines neuen Schlüsselpaares nicht zulässig.

4.6.2 Berechtigte für Antrag auf Neuaustellung Zertifikat / Who may request renewal

Gemäß GLOBALTRUST® Certificate Policy

4.6.3 Bearbeitung eines Antrags auf Neuausstellung Zertifikat / Processing certificate renewal requests

Bei der Neuausstellung von EV Zertifikaten gilt zusätzlich zu den in CPS 4.2 Kriterien das folgende:

Für die Neuausstellung eines EV Zertifikates können die geprüften Daten nur dann ohne neuerliche Prüfung übernommen werden, falls sie nicht älter als 13 Monate sind. Es muss auf jeden Fall jedes ausgestellte EV Zertifikat mit einem eigenen Antrag und einer eigenen Unterschrift der Signaturbedingungen versehen sein (gemäß [CABROWSER-EV] 11.13.1 (4), entspricht Übernahmebestätigung bei Zertifikaten zur fortgeschrittenen Signatur).

Sofern der Antragsteller bereits ein aktuelles und gültiges EV Zertifikat besitzt, dürfen folgende Informationen in jedem Fall ohne neuerliche Prüfung wieder verwendet werden:
- Adresse des Antragstellers
- Telefonnummer des Antragstellers (sofern deren Aktualität durch einen neuerlichen Anruf verifiziert wurde)
- die operative Existenz des Antragstellers

- Name, Titel und Autentizität der handelnden Personen, sofern kein gesonderter Vertrag zwischen dem Antragsteller und dem Betreiber besteht, der eine andere Regelung vorsieht.
- E-Mail Adresse die vom Betreiber für Bestätigungen vom Antragtsteller verwendet wird.
- Das Recht einen Domainnamen zu benützen, sofern dieses in der Vergangenheit durch ein geprüftes Rechtsgutachten oder die Bestätigung eines Wirtschaftsprüfers festgestellt wurde und sich seit damals der Inhaber der Domain (laut WHOIS Eintrag) nicht geändert hat oder der Antragsteller die Verfügungsgewalt neuerlich demonstrieren kann.

4.6.4 Benachrichtigung des Signators über die Neuausstellung Zertifikat / Notification of new certificate issuance to subscriber

Gemäß GLOBALTRUST® Certificate Policy

4.6.5 Verfahren zur Annahme nach Neuausstellung Zertifikat / Conduct constituting acceptance of a renewal certificate

Gemäß GLOBALTRUST® Certificate Policy

4.6.6 Veröffentlichung der Neuausstellung Zertifikat durch ZDA / Publication of the renewal certificate by the CA

Gemäß GLOBALTRUST® Certificate Policy

4.6.7 Benachrichtigung von Dritten über die Ausstellung eines Zertifikates / Notification of certificate issuance by the CA to other entities

Gemäß GLOBALTRUST® Certificate Policy

4.7 Zertifikatsneuausstellung mit Erzeugung eines neuen Schlüsselpaares / Certificate re-key

4.7.1 Umstände für Neuausstellung mit Erzeugung eines neuen Schlüsselpaares / Circumstance for certificate re-key

Gemäß GLOBALTRUST® Certificate Policy

4.7.2 Berechtigung für Antrag auf Neuaustellung mit Erzeugung eines neuen Schlüsselpaares / Who may request certification of a new public key

Gemäß GLOBALTRUST® Certificate Policy

4.7.3 Bearbeitung eines Antrags auf Neuausstellung mit Erzeugung eines neuen Schlüsselpaares / Processing certificate re-keying requests

Gemäß GLOBALTRUST® Certificate Policy

4.7.4 Benachrichtigung über die Neuausstellung eines Zertifikates mit Erzeugung eines neuen Schlüsselpaares / Notification of new certificate issuance to subscriber

Gemäß GLOBALTRUST® Certificate Policy

4.7.5 Verfahren zur Zertifikatsannahme nach Zertifikatsneuausstellung mit Erzeugung eines neuen Schlüsselpaares / Conduct constituting acceptance of a re-keyed certificate

Gemäß GLOBALTRUST® Certificate Policy

4.7.6 Veröffentlichung der Neuausstellung mit Erzeugung eines neuen Schlüsselpaares durch den ZDA / Publication of the re-keyed certificate by the CA

Gemäß GLOBALTRUST® Certificate Policy

4.7.7 Benachrichtigung über die Neuausstellung eines Zertifikates mit Erzeugung eines neuen Schlüsselpaares / Notification of certificate issuance by the CA to other entities

Gemäß GLOBALTRUST® Certificate Policy

4.8 Zertifikatsänderung / Certificate modification

4.8.1 Umstände für Zertifikatsänderung / Circumstance for certificate modification

Gemäß GLOBALTRUST® Certificate Policy

4.8.2 Berechtigte für Antrag auf Zertifikatsänderung / Who may request certificate modification

Gemäß GLOBALTRUST® Certificate Policy

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung / Processing certificate modification requests

Gemäß GLOBALTRUST® Certificate Policy

4.8.4 Benachrichtigung über die Zertifikatsänderung / Notification of new certificate issuance to subscriber

Gemäß GLOBALTRUST® Certificate Policy

4.8.5 Verfahren zur Zertifikatsannahme nach Zertifikatsänderung / Conduct constituting acceptance of modified certificate

Gemäß GLOBALTRUST® Certificate Policy

4.8.6 Veröffentlichung der Zertifikatsänderung / Publication of the modified certificate by the CA

Gemäß GLOBALTRUST® Certificate Policy

4.8.7 Benachrichtigung über die Zertifikatsänderung / Notification of certificate issuance by the CA to other entities

Gemäß GLOBALTRUST® Certificate Policy

4.9 Zertifikatswiderruf und -sperre / Certificate revocation and suspension

4.9.1 Umstände für Zertifikatswiderruf / Circumstances for revocation

Gemäß GLOBALTRUST® Certificate Policy

4.9.2 Berechtigte für Antrag auf Widerruf / Who can request revocation

Gemäß GLOBALTRUST® Certificate Policy

4.9.3 Stellung eines Widerrufantrages / Procedure for revocation request

Gemäß GLOBALTRUST® Certificate Policy

4.9.4 Informationsfrist für Antragstellung auf Widerruf / Revocation request grace period

Gemäß GLOBALTRUST® Certificate Policy

4.9.5 Reaktionszeit des ZDAs auf einen Widerrufsantrag / Time within which CA must process the revocation request

Gemäß GLOBALTRUST® Certificate Policy

4.9.6 Verpflichtung der Nutzer zur Widerrufsprüfung / Revocation checking requirement for relying parties

Gemäß GLOBALTRUST® Certificate Policy

4.9.7 Häufigkeit der Erstellung von Widerrufslisten (CRL) / CRL issuance frequency (if applicable)

Gemäß GLOBALTRUST® Certificate Policy

4.9.8 Maximale Verzögerung der Veröffentlichung der CRLs / Maximum latency for CRLs (if applicable)

Gemäß GLOBALTRUST® Certificate Policy

4.9.9 Möglichkeit der online Widerrufsprüfung / On-line revocation/status checking availability

Die Widerrufsdienste werden insbesondere nach folgenden Standards erbracht: als signierte CRL-Liste gemäß [RFC5280], wobei zur Erstellung Software verwendet wird, die die Vorgaben von [RFC3279] erfüllt oder als OCSP-Dienst nach [RFC2560].

Für Server- und EV-Zertifikate werden die Widerrufsstatusinformationen jedenfall mittels eines OCSP Responders verbreitet.

Jedenfalls in Sperr- bzw. Widerufsliste enthalten sind Datum von Widerruf bzw. Sperre, ein Zeitpunkt für die späteste Veröffentlichung einer Nachfolgeliste sowie eine Signatur vom jeweiligen CA-Zertifikat oder eines davon bestimmten Zertifikates.

Sperr- und Widerrufsinformationen die einen Eintrag mit der OID-Nummer 1.2.40.0.36.4.5.1.0 oder 1.2.40.0.24.4.5.1.0 enthalten, wurden zu Testzwecken erstellt und sind nicht authentisch. Typische Testzwecke sind insbesondere Tests von Neuentwicklungen (Softwaretests), Tests zur Funktionsfähigkeit der Sperr- und Widerrufsdienste. Die Verwendung von Sperren und Widerrufen zu Testzwecken ist auf Zertifikate beschränkt, die zu Testzwecken ausgestellt wurden bzw. Zertifikate die Test-CAs betreffen.

4.9.10 Notwendigkeit der online Widerrufsprüfung / On-line revocation checking requirements

Gemäß GLOBALTRUST® Certificate Policy

4.9.11 Andere verfügbare Widerrufsdienste / Other forms of revocation advertisements available

Gemäß GLOBALTRUST® Certificate Policy

4.9.12 Spezielle Anforderung bei Kompromittierung des privaten Schlüssels / Special requirements re key compromise

Gemäß GLOBALTRUST® Certificate Policy

4.9.13 Umstände für Zertifikatssperre / Circumstances for suspension

Gemäß GLOBALTRUST® Certificate Policy

4.9.14 Berechtigte für Antrag auf Sperre / Who can request suspension

Gemäß GLOBALTRUST® Certificate Policy

4.9.15 Stellung eines Antrages auf Sperre / Procedure for suspension request

Gemäß GLOBALTRUST® Certificate Policy

4.9.16 Dauer einer Zertifikatssperre / Limits on suspension period

Gemäß GLOBALTRUST® Certificate Policy

4.10 Zertifikatsstatusdienste / Certificate status services

4.10.1 Betriebliche Voraussetzungen / Operational characteristics

Gemäß GLOBALTRUST® Certificate Policy

4.10.2 Verfügbarkeit / Service availability

Gemäß GLOBALTRUST® Certificate Policy

4.10.3 Zusätzliche Funktionen / Optional features

Es sind keine zusätzlichen Funktionen definiert.

4.11 Vertragsende / End of subscription

Gemäß GLOBALTRUST® Certificate Policy

4.12 Schlüsselhinterlegung und -wiederherstellung / Key escrow and recovery

4.12.1 Policy und Anwendung von Schlüsselhinterlegung und -wiederherstellung / Key escrow and recovery policy and practices

Gemäß GLOBALTRUST® Certificate Policy

4.12.2 Policy und Anwendung für den Einschluß und die Wiederherstellung von Session keys / Session key encapsulation and recovery policy and practices

Gemäß GLOBALTRUST® Certificate Policy

5. ANFORDERUNGEN STANDORT, MANAGEMENT UND BETRIEB / FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Alle Sicherheitsmaßnahmen und sicherheitsrelevanten Funktionen zur Bereitstellung der Zertifizierungsdienste werden dokumentiert und entsprechend der Dokumentation implementiert und gewartet.

Zur Steuerung des Betriebs wurden für alle Informationen Sicherheitsstufen eingeführt, die zu entsprechend unterschiedlichen betrieblichen Sicherheitsmaßnahmen führen und im GLOBALTRUST® Certificate Policy Abschnitt 9.3 Vertraulichkeit von Geschäftsdaten / Confidentiality of business information detailliert dargestellt sind.

Detailprozesse, insbesondere die Anforderungen zur Installation des Zertifizierungssystems, der Verwaltung der Zertifizierungsdienste und der Verwendung der Zertifizierungssysteme und -dienste werden intern dokumentiert und laufend an betriebliche Anforderungen angepasst.

Anforderungen, die nicht als Geschäftsprozesse technisch installiert werden können, werden durch ein System von Checklisten unterstützt.

Ein Neustart des Zertifizierungssystems (insbesondere der HSM-Module) ist nur am Ort der Installation des HSM-Moduls möglich. Er erfordert sowohl Besitz (Token), als auch Wissen (Initialisierungspasswort). Die erforderlichen Schritte für einen Neustart des Zertifizierungssystems sind intern dokumentiert.

1. Schäden durch sicherheitskritische Zwischenfälle und Fehlfunktionen werden durch ausreichende Aufzeichnungen und Fehlerbehebungsprozeduren frühzeitig erkannt, verhindert oder zumindest minimiert.
2. Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.
3. Für die Ausführung von sicherheitskritischen und administrativen Aufgaben, die sich auf die Erbringung der Zertifizierungsdienste auswirken, sind detaillierte Prozesse in Verwendung.
4. Datenträger werden je nach ihrer Sicherheitsstufe behandelt und gesichert aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.

Die Überwachung der sicherheitskritischen Funktionen obliegt autorisierten Personen gemäß intern dokumentiertem Rollenkonzept des ZDAs oder vom verantwortlichen Dienstleister nominierten Sicherheitsbeauftragten.

Sicherheitsziele und -leitlinien

(1) Zielsetzung und Umsetzung

Die in diesem Abschnitt beschriebene Sicherheitsleitlinie dient zur Erfüllung der rechtlichen und technischen Auflagen bei der Erbringung von Zertifizierungsdiensten durch den Betreiber.

Die zum Betrieb der Zertifizierungsdienste erforderlichen Dokumente und Prozesse werden nachweislich den zuständigen Mitarbeitern zur Kenntnis gebracht. Die Zuständigkeit ergibt sich gemäß internen Rollenkonzept und Rollenzuteilung. Die Gesamtheit der für den Zertifizierungsbetrieb verantwortlichen Mitglieder bilden den Zertifizierungs-Ausschuss.

(2) Identifikation von Risken

Als Risken werden alle Vorgänge und Vorfälle bezeichnet, die zu Unterbrechungen des Betriebs, zur Unterbrechung der Verfügbarkeit kritischer Dienste, oder zu Schädigungen der Vertraulichkeit oder der Integrität von Daten und Anwendungen führen.

Insbesondere davon erfasst sind alle Vorfälle für die der Betreiber gemäß rechtlicher Bestimmungen haftet.

Mitarbeiter sind angehalten Abweichungen und Störungen des Betriebs oder potentielle Sicherheitsprobleme, unabhängig von ihrer formalen Zuständigkeit zu dokumentieren und unverzüglich den zuständigen Stellen (Personen) zu melden. Im Falle unklarer Zuständigkeiten ist der Zertifizierungs-Ausschuss oder die Geschäftsführung zu informieren.

(3) Prinzip der Minimalität

Grundsätzlich werden alle Geschäftsprozesse in Hinblick auf Minimierung von Risken entworfen. Es sollen so wenig Komponenten (Hardware und Software) und Personen als möglich involviert sein.

Weiters werden die Geschäftsprozesse laufend dahingehend optimiert, dass bei Beeinträchtigungen und Schäden die Auswirkungen möglichst lokal begrenzt bleiben.

(4) Prinzip der Authentifikation und Identifikation

Grundsätzlich werden alle Geschäftsprozesse so gestaltet, dass feststellbar ist, welche Personen am Geschäftsprozess beteiligt sind.

Im Zuge der Abwicklung der Geschäftsprozesse müssen sich berechtigte Personen authentifizieren. Soweit einzelne Maßnahmen direkt das Zertifizierungssystem betreffen, führen mehrfach fehlerhafte Authentifikationen zu einer Sperre bzw. falls es sich um eine Authentifikation als Systemadministrator handelt zu einer Information zuständiger Aufsichtspersonen.

Die Zahl der zulässigen Fehlversuche und die Informations- und Benachrichtigungsregeln werden für die Geschäftsprozesse gesondert festgelegt und berücksichtigen die Qualität der verwendeten Identifikationsmechanismen (Passwörter, Schlüssel, Tokens, Smartcard). Grundsätzlich sind Identifikationsmechanismen und zulässige Zahl der Fehlversuche so zu

wählen, dass die Wahrscheinlichkeit von fehlerhaften Identifikationen vernachlässigbar gering ist (weniger als 1:1000).

Die Identifizierung und Authentifizierung kann im Einzelfall durch eine spezifische Systemkomponente erfolgen oder generell auf Basis des darunter liegenden Systems.

Das Zertifizierungssystem unterstützt die Identifizierung und Authentifizierung von zwei Personen ("dual person-control") für Zertifizierungsdienstleistungen die gemäß anzuwendender Certificate Policy das Vier-Augen-Prinzip erfordern.

(5) Prinzip der Vertraulichkeit

Alle kritischen Informationen, Prozesse und Systeme unterliegen einer Zugangsbeschränkung. Diese wird durch physikalische Zutrittsbeschränkungen zu den Systemen, durch generelle Zugriffsbeschränkungen bzw. individuelle Zugriffsprofile sichergestellt.

Im Falle der zentralen Zertifizierungsdienste erfolgt die Beschränkung durch eine Kombination der genannten Maßnahmen.

Persönliche Informationen der Antragsteller oder Dritter werden vertraulich behandelt, es sei denn der Zweck eines Zertifizierungsdienstes sieht ausdrücklich etwas anderes vor. Keine vertraulichen Informationen sind zur Veröffentlichung freigegebene Zertifikate und deren Inhalte. Keiner Vertraulichkeit unterliegen Angaben über den Zeitpunkt und Identifikationsdaten widerrufener Zertifikate.

(6) Prinzip der Aktualität

Kritische Teile der Geschäftsprozesse werden laufend auf ihre Aktualität und Angemessenheit in Hinblick auf den Stand der Technik geprüft.

Dazu werden Mitteilungen der Aufsichtstelle, Mitteilungen der Hersteller, nationale und internationale CERT-Informationen, Rückmeldungen von Kunden und Fachpublikationen herangezogen. Regelmäßig wird jeder Geschäftsprozess systematisch in Hinblick auf bisher nicht erkannte Risken und Schwachstellen untersucht und optimiert. Die Prüffrequenz richtet sich nach den betrieblichen Erfordernissen und den potentiellen Risken jedes Geschäftsprozesses und liegt in einem Zeitraum von 12 bis 18 Monaten.

(7) Prinzip von Redundanz und Fail-Safe (Notfallleitlinie)

Kritische Geschäftsprozesse, Systeme und Tätigkeiten sind redundant ausgeführt. Das Design der Prozesse ist zusätzlich so ausgelegt, dass bei Störungen, die nicht im Rahmen dokumentierter Verfahren behebbar sind, Eskalationsstrategien verwendet werden, die am Ende auch zur Abschaltung angebotener Dienste führen können.

Bei Ausfall einzelner, redundant ausgeführter Komponenten kann es zur verminderten Verfügbarkeit kommen. Anfragen bzw. Anforderungen an diese Dienste müssen, abhängig von der eingesetzen Clientsoftware (z.B. Browser, Reader, Signaturprüfprogramme), um erfolgreich zu sein, unter Umständen mehrfach erfolgen.

Bei der Umsetzung der Eskalationsstrategien sind alle Mitglieder des Zertifizierungs-Ausschusses eingebunden.

(8) Wartungsvereinbarung

Zu kritischen Komponenten existieren Wartungsvereinbarungen, die einen Ersatz schadhafter Komponenten innerhalb eines Zeitraums erlauben, der kürzer ist als die übliche durchschnittliche Ausfallszeitwahrscheinlichkeit einer Komponente. Kritische Komponenten sind jene Komponenten, die auf Grund ihrer Bauart und/oder Komplexität nicht kurzfristig im allgemeinen Handel beschaft werden können.

In der Kombination von Redundanz und Wartungsvereinbarung ist für abschätzbare Risken gesichert, dass zumindest eine Komponente für den regulären Betrieb zur Verfügung steht.

Für nicht-kritische Komponenten wurden für Ausfälle organisatorische Vorkehrungen zur Aufrechterhaltung des Betriebs getroffen.

(9) Prinzip der Auslagerung

Nicht vermeidbare Restrisken, die weder technisch noch organisatorisch gelöst werden können, werden durch "Auslagerung" verhindert oder zumindest reduziert.

Dazu zählt in erster Linie der Abschluss einer Haftpflichtversicherung.

Weiters werden besondere Bereitschaftszeiten, spezielle Fachkenntnisse oder Betriebserfordernisse durch Beiziehung geeigneter Spezialisten abgedeckt. Bei Beiziehung sind Anbieter mit einschlägigen Zertifizierungen, bei ansonsten gleichen Voraussetzungen, grundsätzlich zu bevorzugen. Die Liste geeigneter Spezialisten und mit ihnen abgeschlossene Vereinbarungen ist intern dokumentiert, die tatsächlich herangezogenen Spezialisten werden intern protokolliert.

(10) Prinzip der Risikoakzeptanz

Die in dieser Leitline beschriebenen Prinzipien werden in der GLOBALTRUST® Certificate Security Policy für alle Dienste des ZDA beschrieben und bewertet. Die Risikoanalyse verwendet in diesem Zusammenhang die Schutzbedarfskategorisierung "normal", "hoch" und "sehr hoch" gemäß [BSI-GRUND]. Alle nach Umsetzung der in der GLOBALTRUST® Certificate Security Policy beschriebenen Maßnahmen verbleibenden Restrisiken der Schutzbedarfskategorie "normal" werden ausdrücklich von der Geschäftsführung des ZDA zur Kenntnis genommen und akzeptiert.

Risken die darüber hinaus gehen und etwa als "hoch" oder "sehr hoch" eingestuft werden, werden durch Zusatzmaßnahmen soweit minimiert, dass das Risiko akzeptabel ist. Die Maßnahmen zur Minimierung der Risken sind in der GLOBALTRUST® Certificate Security Policy beschrieben. Verbleibende Restrisken werden ausdrücklich von der Geschäftsführung des ZDA zur Kenntnis genommen und akzeptiert.

5.1 Bauliche Sicherheitsmaßnahmen / Physical controls

Insbesondere gelten folgende Sicherheitsmaßnahmen:

1. Die Systeme für die Zertifikatsgenerierung und die Widerrufsdienste werden durch technische und organisatorische Maßnahmen in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe verhindert wird.

2. Die Abgrenzung der Systeme für Zertifikatsgenerierung, Erstellung von Signaturerstellungseinheiten und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen sowie physischen Zutrittsschutz.
3. Die Sicherheitsmaßnahmen beinhalten den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung und Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten sowie vor Diebstahl, Einbruch und Systemausfällen.
4. Die unautorisierte Entnahme von Informationen, Datenträgern, Software und Einrichtungsgegenständen, welche zu den Zertifizierungsdiensten gehören, wird durch Kontrollmaßnahmen verhindert.

Gegen physikalische Störungen bestehen technische, bauliche und organisatorische Sicherungsmaßnahmen wie redundante Systemführungen, Notstromaggregate, Brandschutz.

5.1.1 Standortlage und Bauweise / Site location and construction

Alle kritischen IT-Komponenten für die Erbringung von Zertifizierungsdiensten, inklusive der Ausstellung qualifizierter Zertifikate und qualifizierter Zeitstempel, sind in einem Rechenzentrum ausgelagert, dass eine ISO 27001-Zertifizierung, eine gleichwertige Zertifizierung oder eine gleichwertiges individuelles Sicherheitskonzept, das dem Stand der Technik entspricht, vorweist.

Der aktuelle Standort und die eingesetzten IT-Komponenten sind intern dokumentiert, die einzelnen Sicherheitsmaßnahmen insbesondere der Schutz der technischen Komponenten vor unbefugten Veränderungen im Dokument GLOBALTRUST® Certificate Security Policy.

5.1.2 Zutritt / Physical access

Gemäß GLOBALTRUST® Certificate Policy

5.1.3 Stromnetz und Klimaanlage / Power and air conditioning

Gemäß GLOBALTRUST® Certificate Policy

5.1.4 Gefährdungspotential durch Wasser / Water exposures

Gemäß GLOBALTRUST® Certificate Policy

5.1.5 Brandschutz / Fire prevention and protection

Gemäß GLOBALTRUST® Certificate Policy

5.1.6 Aufbewahrung von Speichermedien / Media storage

Gemäß GLOBALTRUST® Certificate Policy

5.1.7 Abfallentsorgung / Waste disposal

Gemäß GLOBALTRUST® Certificate Policy

5.1.8 Offsite Backup / Off-site backup

Gemäß GLOBALTRUST® Certificate Policy

5.2 Prozessanforderungen / Procedural controls

5.2.1 Rollenkonzept / Trusted roles

Gemäß GLOBALTRUST® Certificate Policy

5.2.2 Mehraugenprinzip / Number of persons required per task

Gemäß GLOBALTRUST® Certificate Policy

5.2.3 Identifikation und Authentifikation der Rollen / Identification and authentication for each role

Gemäß GLOBALTRUST® Certificate Policy

5.2.4 Rollenausschlüsse / Roles requiring separation of duties

Gemäß GLOBALTRUST® Certificate Policy

5.3 Mitarbeiteranforderungen / Personnel controls

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit / Qualifications, experience, and clearance requirements

Gemäß GLOBALTRUST® Certificate Policy

5.3.2 Durchführung von Backgroundchecks / Background check procedures

Gemäß GLOBALTRUST® Certificate Policy

5.3.3 Schulungen/ Training requirements

Gemäß GLOBALTRUST® Certificate Policy

5.3.4 Häufigkeit von Schulungen und Anforderungen / Retraining frequency and requirements

Gemäß GLOBALTRUST® Certificate Policy

5.3.5 Häufigkeit und Abfolge Arbeitsplatzrotation / Job rotation frequency and sequence

Gemäß GLOBALTRUST® Certificate Policy

5.3.6 Strafmaßnahmen für unerlaubte Handlungen / Sanctions for unauthorized actions

Gemäß GLOBALTRUST® Certificate Policy

5.3.7 Anforderungen an Dienstleister / Independent contractor requirements

Gemäß GLOBALTRUST® Certificate Policy

5.3.8 Zu Verfügung gestellte Unterlagen / Documentation supplied to personnel

Gemäß GLOBALTRUST® Certificate Policy

5.4 Betriebsüberwachung / Audit logging procedures

Zur Qualitätssicherung werden regelmäßig Selbst-Audits durchgeführt. Bei EV- und Server-Zertifikaten werden zumindest 3% (mindestens eines) aller seit dem letzten Selbst-Audit ausgestellten Zertifikate überprüft sowie 6% aller EV-Zertifkate und 3% aller Serverzertifikate, bei welchen die Identitäts- oder Endprüfung von einem Dienstleister durchgeführt wurde. Die Selbst-Audits für Server-Zertifikate erfolgen zumnidest einmal pro Quartal.

Der ZDA verpflichtet sich einmal im Quartal eine Prüfung von mindestens 3% (mindestens eines) aller der in diesem Quartal ausgestellter, technisch eingeschränkter Sub-Zertifikate, deren privater Schlüssel sich nicht unter der alleinigen Kontrolle des ZDA befindet ausgestellten Zertifikaten auf Einhaltung aller anwendbarer Bestimmungen, insbesondere von [CABROWSER-BASE], durchzuführen.

Betriebsüberwachung, Bereitschaftsdienst und Protokollierung besonderer Betriebssituationen
Der reguläre Betrieb des Zertifizierungssystems unterliegt einer laufenden, automationsunterstützten Betriebsüberwachung, die mehrere Interfaces aufweist. Unter anderem kann der Betriebszustand jederzeit über Web-Interfaces von befugten Personen kontrolliert werden. Bei bestimmten Ereignissen erfolgt eine automatisierte Benachrichtigung der verantwortlichen Stellen. Diese Benachrichtigung kann per eMail, SMS oder anderer geeigneter Signal- oder Nachrichtendienste erfolgen.

Das Überwachungsystem selbst ist so ausgeführt, dass die Überwachung - soweit technisch sinnvoll - direkt an den entsprechenden Standorten erfolgt, die Funktionsfähigkeit des jeweiligen lokalen Überwachungssystems selbst wird durch ein anderes, externes Überwachungssystem überwacht.

Sofern ein Überwachungssystem dauerhaft nicht verfügbar ist, sind für die kritischen Prozesse manuelle Überwachungsmaßnahmen vorgesehen. Die Art der Maßnahmen ist intern dokumentiert.

5.4.1 Zu erfassende Ereignisse / Types of events recorded

Gemäß GLOBALTRUST® Certificate Policy

5.4.2 Überwachungsfrequenz / Frequency of processing log

Gemäß GLOBALTRUST® Certificate Policy

5.4.3 Aufbewahrungsfrist für Überwachungsaufzeichungen / Retention period for audit log

Gemäß GLOBALTRUST® Certificate Policy

5.4.4 Schutz der Überwachungsaufzeichnungen / Protection of audit log

Gemäß GLOBALTRUST® Certificate Policy

5.4.5 Sicherung des Archives der Überwachungsaufzeichnungen / Audit log backup procedures

Gemäß GLOBALTRUST® Certificate Policy

5.4.6 Betriebsüberwachungssystem/ Audit collection system (internal vs. external)

Gemäß GLOBALTRUST® Certificate Policy

5.4.7 Benachrichtigung des Auslösers / Notification to event-causing subject

Nicht zutreffend

5.4.8 Gefährdungsanalyse / Vulnerability assessments

Gemäß GLOBALTRUST® Certificate Policy

5.5 Aufzeichnugsarchivierung / Records archival

Der Zertifizierungsantrag und alle damit im Zusammenhang stehenden vom Antragsteller zugesandten und vorliegenden Daten und Dokumente (Ausweiskopien, gegebenenfalls Bestätigungen über das Unternehmen und die Vertretungsbefugnis) sowie alle zum Zertifikat geschlossenen Vereinbarungen und Verträge werden auf die Dauer von mind. 35 Jahren nach Ablauf der Gültigkeit elektronisch oder in Papierform in dem Umfang archiviert, dass die ursprüngliche Antragstellung, Zertifikatsausstellung und Zertifikatszustellung nachvollzogen werden können.

5.5.1 Zu archivierende Aufzeichungen / Types of records archived

Gemäß GLOBALTRUST® Certificate Policy

5.5.2 Aufbewahrungsfristen für archivierte Daten / Retention period for archive

Gemäß GLOBALTRUST® Certificate Policy

5.5.3 Schutz der Archive / Protection of archive

Gemäß GLOBALTRUST® Certificate Policy

5.5.4 Sicherung des Archives / Archive backup procedures

Gemäß GLOBALTRUST® Certificate Policy

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen / Requirements for time-stamping of records

Gemäß GLOBALTRUST® Certificate Policy

5.5.6 Archivierung (intern/extern) / Archive collection system (internal or external)

Gemäß GLOBALTRUST® Certificate Policy

5.5.7 Verfahren zur Beschaffung und Verifikation von Aufzeichungen / Procedures to obtain and verify archive information

Gemäß GLOBALTRUST® Certificate Policy

5.6 Schlüsselwechsel des Betreibers / Key changeover

Gemäß GLOBALTRUST® Certificate Policy

5.7 Kompromittierung und Geschäftsweiterführung / Compromise and disaster recovery

5.7.1 Handlungsablauf bei Zwischenfällen und Kompromittierungen / Incident and compromise handling procedures

Gemäß GLOBALTRUST® Certificate Policy

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen / Computing resources, software, and/or data are corrupted

Gemäß GLOBALTRUST® Certificate Policy

5.7.3 Handlungsablauf Kompromittierung des privaten Schlüssels des ZDA / Entity private key compromise procedures

Gemäß GLOBALTRUST® Certificate Policy

5.7.4 Möglichkeiten zur Geschäftsweiterführung im Katastrophenfall / Business continuity capabilities after a disaster

Gemäß GLOBALTRUST® Certificate Policy

5.8 Einstellung der Tätigkeit / CA or RA termination

Gemäß GLOBALTRUST® Certificate Policy

6. TECHNISCHE SICHERHEITSMAßNAHMEN / TECHNICAL SECURITY CONTROLS

6.1 Erzeugung und Installation von Schlüsslpaaren / Key pair generation and installation

6.1.1 Erzeugung von Schlüsselpaaren/ Key pair generation

Erzeugung der privaten Schlüssel und des Zertifikates zu den CA-Zertifikaten

Die Erstellung eines privaten Schlüssels für ein -Zertifikat, welcher nach dem 9.7.2013 erstellt wurde und für die Ausstellung von EV-Zertifikaten verwendet wird, wird von einer kompetenten und unabhängigen Auditstelle überwacht.

Erzeugung der privaten Schlüssel des Signators

Werden für die Signaturerstellungseinheit spezielle Hardwarekomponenten verwendet die das Auslesen des privaten Schlüssels verhindern, können diese von Bestätigungsstellen evaluiert (zertifiziert) sein. Alternativ kann die Eignung durch Selbstdeklaration des Herstellers gegeben sein. Welchen Kriterien und Standards eine Signaturerstellungseinheit genügt wird vom Betreiber dokumentiert und kann über dessen Website oder auf Anfrage abgerufen werden.

Die Verwendung derartiger Signaturerstellungseinheiten kann als X.509v3-Erweiterung im Zertifikat eingetragen werden.

Der Eintrag kann in folgender Form erfolgen:
- Bereitstellung des Schlüssels durch den Betreiber
- Schlüsselgenerierung beim Signator
- Schlüsselgenerierung durch befugte Dritte

a. Bereitstellung des Schlüssels durch den ZDA

Variante I: Erzeugen des Schlüssels in einer sicheren Signaturerstellungseinheit
Der private Schlüssel des Signators wird vom ZDA in einer dafür speziell geeigneten Signaturerstellungseinheit generiert und nur in dieser Signaturerstellungeinheit ausgeliefert. Beim ZDA existiert keine Kopie des privaten Schlüssels außerhalb der Signaturerstellungseinheit.

Ein X.509v3-Zertifikat kann folgenden Erweiterung enthalten:
1.2.40.0.36.4.1.1: <verwendete Hardware>

Unter "<verwendete Hardware>" wird die handelsübliche oder durch eine Bestätigungsstelle verwendete Bezeichnung zur eindeutigen Kennzeichnung der Hardware verwendet, z.B. "Safenet eToken Pro64k" für einen USB-Token mit der evaluierten Komponente "CardOS V4.2 CNS with Application for Digital Signature" der Firma ATOS.

Der aktuelle Stand der unterstützten Hardwarekomponenten und welche Bestätigungsstellen nach welchen gesetzlichen Bestimmungen die Evaluation durchführten, findet sich auf der Website des ZDA.

Wird das Zertifikat im Verzeichnisdienst des ZDA veröffentlicht wird in den Stammdaten zusätzlich die verwendete Hardware unter der Bezeichnung "globaltrustIssuerInfo" eingetragen.

Diese Variante ist für qualifizierte und einfache Zertifikate möglich.

Variante II: Erzeugen des Schlüssels für den Signator in einer gesicherten Zertifizierungsumgebung

Der private Schlüssel des Signators wird vom ZDA in einer dafür speziell betrieben Signaturerstellungsumgebung erstellt und wird zur Übergabe mit einem vom Signator vergebenen Passwort verschlüsselt.

Diese Variante ist nur für einfache Zertifikate möglich.

b. Schlüsselgenerierung beim Signator

Der Signator gibt an, mit welcher Hardware er den privaten Schlüssel generiert hat.

Wird das Zertifikat im Verzeichnisdienst des ZDAs veröffentlicht wird in den Stammdaten zusätzlich die verwendete Hardware unter der Bezeichnung "globaltrustSignerInfo" eingetragen.

Diese Variante ist nur für einfache Zertifikate möglich.

c. Schlüsselgenerierung durch befugte Dritte

Bedingungen wie ⇨ a. Bereitstellung des Schlüssels durch den ZDA (p42), die Schlüsselgenerierung erfolgt jedoch durch ausreichend befugte Dritte, z.B. Ziviltechniker, die die ordnungsgemäße Generierung des privaten Schlüssels bestätigen.

Diese Variante ist für qualifizierte und einfache Zertifikate möglich.

5. Abschluss

Fehlen beide X509v3-Erweiterungen und enthält das Zertifikat keinen Eintrag als qualifiziertes Zertifikat, dann gelten jedenfalls die Aufbewahrungsbestimmungen für den privaten Schlüssel gemäß ⇨ GLOBALTRUST® Certificate Policy Abschnitt "Ergänzende Bestimmungen bei Einsatz auslesbarer Datenträger für private Schlüssel".

6.1.2 Zustellung privater Schlüssel an den Signator / Private key delivery to subscriber

Gemäß GLOBALTRUST® Certificate Policy

6.1.3 Zustellung öffentlicher Schlüssel an den ZDA / Public key delivery to certificate issuer

Gemäß GLOBALTRUST® Certificate Policy

6.1.4 Verteilung öffentliche CA-Schlüssel / CA public key delivery to relying parties

Gemäß GLOBALTRUST® Certificate Policy

6.1.5 Schlüssellängen / Key sizes

Gemäß GLOBALTRUST® Certificate Policy

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle / Public key parameters generation and quality checking

Gemäß GLOBALTRUST® Certificate Policy

6.1.7 Schlüsselverwendung / Key usage purposes (as per X.509 v3 key usage field)

Gemäß GLOBALTRUST® Certificate Policy

6.2 Schutz des privaten Schlüssels und Anforderungen an Signaturerstellungseinheiten / Private Key Protection and Cryptographic Module Engineering Controls

Schlüssel für qualifizierte Zertifikate werden nur auf sicheren Signaturerstellungseinheiten ausgestellt.

6.2.1 Standards und Sicherheitsmaßnahmen für Signaturerstellungseinheiten / Cryptographic module standards and controls

Für Schlüssel, die für fortgeschrittene Signaturen vorgesehen sind werden alle Produkte, die zumindest eine Zertifizierung gemäß [CC-ITSE] EAL4+ oder gemäß [FIPS-140-2] L1 aufweisen.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m) / Private key (n out of m) multi-person control

Gemäß GLOBALTRUST® Certificate Policy

6.2.3 Hinterlegung privater Schlüssel (key escrow) / Private key escrow

Gemäß GLOBALTRUST® Certificate Policy

6.2.4 Backup privater Schlüssel / Private key backup

Gemäß GLOBALTRUST® Certificate Policy

6.2.5 Archivierung privater Schlüssel / Private key archival

Die privaten Schlüssel des Signators werden, sofern sie vom Betreiber erstellt wurden und Kopien vorhanden sind, nach Abruf durch den Signator und der Bestätigung des korrekten Empfangs durch den Signator, beim Betreiber gelöscht.

6.2.6 Transfer privater Schlüssel in oder aus Signaturerstellungseinheiten / Private key transfer into or from a cryptographic module

Gemäß GLOBALTRUST® Certificate Policy

6.2.7 Speicherung privater Schlüssel auf Signaturerstellungseinheiten / Private key storage on cryptographic module

Gemäß GLOBALTRUST® Certificate Policy

6.2.8 Aktivierung privater Schlüssel / Method of activating private key

Gemäß GLOBALTRUST® Certificate Policy

6.2.9 Deaktivierung privater Schlüssel / Method of deactivating private key

Gemäß GLOBALTRUST® Certificate Policy

6.2.10 Zertstörung privater Schlüssel / Method of destroying private key

Gemäß GLOBALTRUST® Certificate Policy

6.2.11 Beurteilung Signaturerstellungseinheiten / Cryptographic Module Rating

Gemäß GLOBALTRUST® Certificate Policy

6.3 Andere Aspekte des Managements von Schlüsselpaaren / Other aspects of key pair management

6.3.1 Archvierung eines öffentlichen Schlüssels / Public key archival

Gemäß GLOBALTRUST® Certificate Policy

6.3.2 Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren / Certificate operational periods and key pair usage periods

Gemäß GLOBALTRUST® Certificate Policy

6.4 Aktivierungsdaten / Activation data

6.4.1 Generierung und Installation von Aktivierungsdaten / Activation data generation and installation

Gemäß GLOBALTRUST® Certificate Policy

6.4.2 Schutz von Aktivierungsdaten / Activation data protection

Gemäß GLOBALTRUST® Certificate Policy

6.4.3 Andere Aspekte von Aktivierungsdaten / Other aspects of activation data

Gemäß GLOBALTRUST® Certificate Policy

6.5 Sicherheitsmaßnahmen IT-System / Computer security controls

Gemäß GLOBALTRUST® Certificate Policy

6.5.1 Spezifische technische Sicherheitsanforderungen an die IT-Systeme / Specific computer security technical requirements

Gemäß GLOBALTRUST® Certificate Policy

6.5.2 Beurteilung der Computersicherheit / Computer security rating

Gemäß GLOBALTRUST® Certificate Policy

6.6 Technische Maßnahmen während des Lebenszyklus / Life cycle technical controls

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung / System development controls

Gemäß GLOBALTRUST® Certificate Policy

6.6.2 Sicherheitsmaßnahmen beim Computermanagement / Security management controls

Gemäß GLOBALTRUST® Certificate Policy

6.6.3 Sicherheitsmaßnahmen während des Lebenszyklus / Life cycle security controls

Gemäß GLOBALTRUST® Certificate Policy

6.7 Sicherheitsmaßnahmen Netzwerke / Network security controls

Die erforderlichen Sicherheitsmaßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.8 Zeitstempel / Time-stamping

Die für die Zertifizierungsdienste relevanten Systeme sind zeitlich untereinander synchronisiert und werden laufend mit der "Universal Time Coordinated (UTC)" abgeglichen.

Zu diesem Zweck wird das Protokoll NTP [RFC5905] oder ein gleichwertiges Protokoll herangezogen, das als verlässlicher Mechanismus zum Zeitabgleich anerkannt ist. Der

Zeitabgleich erfolgt über öffentlich verfügbare NTP-Server anerkannter Einrichtungen, wie z.B. die deutsche Physikalisch-Technische Bundesanstalt oder sonstiger technischer Systeme, die standardisierte Zeitwerte direkt empfangen können. Insbesondere sind dies DCF77-Zeitformat, das GPS-Zeitformat oder vergleichbare, verwandte satellitengestützte Positionierungssysteme mit vergleichbar genauen Zeitangaben (Synchronzeit). Es werden zumindest zwei unabhängige Zeitquellen herangezogen, die korrekte Zeit wird durch Abgleich der unterschiedlichen Quellen ermittelt und erlaubt die Synchronisation der Zeiten für die Zertifizierungsdienste mit der "Universal Time Coordinated (UTC)" innerhalb einer Sekunde. Diese Genauigkeit gilt insbesondere für die Zeitquelle des Zeitstempeldienstes.

Der Ausfall einer oder mehrerer Zeitquellen wird durch die Betriebsüberwachung erkannt und dokumentiert. Ausfälle, die eine größere Zeitabweichung als die durch die Aufsichtstellen vorgegebene akzeptable Abweichung erwarten lassen, führen zum Stopp aller Zertifizierungsdienste die eine exakte Zeitangabe erfordern, insbesondere der Zeitstempeldienste, der Signatur des OCSP-Response und der Signatur der Widerrufs- und Sperrlisten.

Zur Sicherung der Genauigkeit wird die Synchronzeit regelmäßig mit der Systemzeit des Systems, das die Zeitstempel erstellt, synchronisiert. Dazu wird zumindest einmal täglich die Systemzeit mit der Synchronzeit verglichen und allfällige Abweichungen gemäß [RFC5905] oder gleichwertig eliminiert .

Der Betreiber behält sich vor, zusätzliche Verfahren zur Sicherung der korrekten Zeit heranzuziehen.

Zur Dokumentation der Zeitgenauigkeit werden laufend Statistiken über die beobachteten Abweichungen und die Verfügbarkeit der Synchronzeiten durchgeführt.

Zeitstempel die einen Eintrag mit der OID-Nummer 1.2.40.0.36.4.5.2.0 oder 1.2.40.0.24.4.5.2.0 enthalten, wurden zu Testzwecken erstellt und sind nicht authentisch, insbesondere können die Zeitangaben von den Vorgaben dieser Policy oder dem GLOBALTRUST® Certificate Practice Statement abweichen. Typische Testzwecke sind insbesondere Tests von Neuentwicklungen (Softwaretests) und Tests zur Funktionsfähigkeit der Zeitstempeldienste.

7. PROFILE DER ZERTIFIKATE, WIDERRUFSLISTEN UND OCSP / CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Zertifikatsprofile / Certificate profile

7.1.1 Versionsnummern / Version number(s)

Gemäß GLOBALTRUST® Certificate Policy

7.1.2 Zertifikatserweiterungen / Certificate extensions

Testzertifikate im X509v3-Format können mit der Erweiterung 1.2.40.0.36.4.1.0=DER:01:01:FF (Testeigenschaft = TRUE ausgezeichnet werden. **Diese Erweiterung ist nicht für qualifizierte Zertifikate erlaubt.**

7.1.3 Algorithmen OIDs / Algorithm object identifiers

Gemäß GLOBALTRUST® Certificate Policy

7.1.4 Namensformate / Name forms

Gemäß GLOBALTRUST® Certificate Policy

7.1.5 Namensbeschränkungen / Name constraints

Gemäß GLOBALTRUST® Certificate Policy

7.1.6 Certificate Policy Object Identifier / Certificate policy object identifier

Gemäß GLOBALTRUST® Certificate Policy

7.1.7 Nutzung der Erweiterung „PolicyConstraints" / Usage of Policy Constraints extension

Gemäß GLOBALTRUST® Certificate Policy

7.1.8 Syntax und Semantik von „PolicyQualifiers" / Policy qualifiers syntax and semantics

Gemäß GLOBALTRUST® Certificate Policy

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung CertificatePolicies / Processing semantics for the critical Certificate Policies extension

Gemäß GLOBALTRUST® Certificate Policy

7.2 Sperrlistenprofile / CRL profile

Gemäß GLOBALTRUST® Certificate Policy

7.2.1 Versionsnummern / Version number(s)

Gemäß GLOBALTRUST® Certificate Policy

7.2.2 Erweiterungen von Widerrufslisten und Widerrufslisteneinträgen / CRL and CRL entry extensions

Gemäß GLOBALTRUST® Certificate Policy

7.3 Profile des Statusabfragedienstes (OCSP) / OCSP profile

7.3.1 Versionsnummern / Version number(s)

Gemäß GLOBALTRUST® Certificate Policy

7.3.2 OCSP-Erweiterungen / OCSP extensions

Gemäß GLOBALTRUST® Certificate Policy

8. PRÜFUNG DER KONFORMITÄT UND ANDERE BEURTEILUNGEN / COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Häufigkeit und Umstände für Beurteilungen / Frequency or circumstances of assessment

Gemäß GLOBALTRUST® Certificate Policy

8.2 Identifikation/Qualifikation des Gutachters / Identity/qualifications of assessor

Gemäß GLOBALTRUST® Certificate Policy

8.3 Beziehung des Gutachters zur zu überprüfenden Einrichtung / Assessor's relationship to assessed entity

Gemäß GLOBALTRUST® Certificate Policy

8.4 Behandelte Themen der Beurteilung / Topics covered by assessment

Gemäß GLOBALTRUST® Certificate Policy

8.5 Handlungsablauf bei negitivem Ergebnis / Actions taken as a result of deficiency

Gemäß GLOBALTRUST® Certificate Policy

8.6 Mitteilung des Ergebnisses / Communication of results

Gemäß GLOBALTRUST® Certificate Policy

9. REGELUNGEN FÜR SONSTIGE FINANZIELLE UND GESCHÄFTLICHE ANGELEGENHEITEN / OTHER BUSINESS AND LEGAL MATTERS

9.1 Kosten / Fees

Gemäß GLOBALTRUST® Certificate Policy

9.1.1 Kosten für Zertifikatsaustellung und -erneuerung / Certificate issuance or renewal fees

Gemäß GLOBALTRUST® Certificate Policy

9.1.2 Kosten für den Zugriff auf Zertifikate / Certificate access fees

Gemäß GLOBALTRUST® Certificate Policy

9.1.3 Kosten für Widerruf oder Statusinformationen / Revocation or status information access fees

Gemäß GLOBALTRUST® Certificate Policy

9.1.4 Kosten für andere Dienstleistungen / Fees for other services

Gemäß GLOBALTRUST® Certificate Policy

9.1.5 Kostenrückerstattung / Refund policy

Gemäß GLOBALTRUST® Certificate Policy

9.2 Finanzielle Verantwortung / Financial responsibility

Gemäß GLOBALTRUST® Certificate Policy

9.2.1 Versicherungsdeckung / Insurance coverage

Gemäß GLOBALTRUST® Certificate Policy

9.2.2 Andere Ressourcen für Betriebserhaltung und Schadensdeckung / Other assets

Gemäß GLOBALTRUST® Certificate Policy

9.2.3 Versicherung oder Gewährleistung für Endnutzer / Insurance or warranty coverage for end-entities

Gemäß GLOBALTRUST® Certificate Policy

9.3 Vertraulichkeit von Geschäftsdaten / Confidentiality of business information

9.3.1 Definition vertrauliche Geschäftsdaten / Scope of confidential information

Gemäß GLOBALTRUST® Certificate Policy

9.3.2 Geschäftsdaten, die nicht vertraulich behandelt werden / Information not within the scope of confidential information

Gemäß GLOBALTRUST® Certificate Policy

9.3.3 Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten / Responsibility to protect confidential information

Gemäß GLOBALTRUST® Certificate Policy

9.4 Datenschutz von Personendaten / Privacy of personal information

9.4.1 Datenschutzkonzept / Privacy plan

Gemäß GLOBALTRUST® Certificate Policy

9.4.2 Definition von Personendaten / Information treated as private

Gemäß GLOBALTRUST® Certificate Policy

9.4.3 Daten, die nicht vertraulich behandelt werden / Information not deemed private

Gemäß GLOBALTRUST® Certificate Policy

9.4.4 Zuständigkeiten für den Datenschutz / Responsibility to protect private information

Gemäß GLOBALTRUST® Certificate Policy

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten / Notice and consent to use private information

Gemäß GLOBALTRUST® Certificate Policy

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften / Disclosure pursuant to judicial or administrative process

Gemäß GLOBALTRUST® Certificate Policy

9.4.7 Andere Bedingungen für Auskünfte / Other information disclosure circumstances

Gemäß GLOBALTRUST® Certificate Policy

9.5 Schutz-und Urheberrechte / Intellectual property rights

Der Betreiber bietet Zertifizierungsdienste unter der Markenbezeichnung GLOBALTRUST® an.

GLOBALTRUST® ist eine EU-weit unter der Nummer 002286649 eingetragene Gemeinschaftsmarke (http://oami.europa.eu) des in Österreich eingetragenen Vereins "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (ZVR 774004629), in Folge kurz "Verein". Die Nutzungsrechte der Marke GLOBALTRUST® für Zertifizierungsdienste und insbesondere die Nutzung folgender Root-Zertifikate zur Zertifizierung (insbesondere Signatur) von Zertifikaten und Signaturerstellungsdaten des ZDA, des Vereins oder Dritter und wird dem ZDA vom Verein uneingeschränkt und auf unbestimmte Zeit eingeräumt.

9.6 Zusicherungen und Garantien / Representations and warranties

9.6.1 Leistungsumfang des ZDA / CA representations and warranties

Gemäß GLOBALTRUST® Certificate Policy

9.6.2 Leistungsumfang der Registrierungsstellen / RA representations and warranties

Gemäß GLOBALTRUST® Certificate Policy

9.6.3 Zusicherungen und Garantien des Signators / Subscriber representations and warranties

Gemäß GLOBALTRUST® Certificate Policy

9.6.4 Zusicherungen und Garantien des Zertifikatsnutzers / Relying party representations and warranties

Gemäß GLOBALTRUST® Certificate Policy

9.6.5 Zusicherungen und Garantien anderer Teilnehmer / Representations and warranties of other participants

Gemäß GLOBALTRUST® Certificate Policy

9.7 Haftungsausschlüsse / Disclaimers of warranties

Gemäß GLOBALTRUST® Certificate Policy

9.8 Haftungsbeschränkungen / Limitations of liability

Gemäß GLOBALTRUST® Certificate Policy

9.9 Schadensersatz / Indemnities

Gemäß GLOBALTRUST® Certificate Policy

9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit / Term and termination

9.10.1 Gültigkeitsdauer der CP / Term

Gemäß GLOBALTRUST® Certificate Policy

9.10.2 Beendigung der Gültigkeit / Termination

Gemäß GLOBALTRUST® Certificate Policy

9.10.3 Auswirkung der Beendigung / Effect of termination and survival

Gemäß GLOBALTRUST® Certificate Policy

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern / Individual notices and communications with participants

Gemäß GLOBALTRUST® Certificate Policy

9.12 Änderungen / Amendments

9.12.1 Verfahren bei Änderungen / Procedure for amendment

Gemäß GLOBALTRUST® Certificate Policy

9.12.2 Benachrichtigungsmechanismen und –fristen / Notification mechanism and period

Gemäß GLOBALTRUST® Certificate Policy

9.12.3 Bedingungen für OID-Änderungen / Circumstances under which OID must be changed

Gemäß GLOBALTRUST® Certificate Policy

9.13 Bestimmungen zur Schlichtung von Streitfällen / Dispute resolution provisions

Gemäß GLOBALTRUST® Certificate Policy

9.14 Gerichtsstand / Governing law

Gemäß GLOBALTRUST® Certificate Policy

9.15 Einhaltung geltenden Rechts / Compliance with applicable law

Das GLOBALTRUST® Certificate Practice Statement gilt für alle Zertifikate, die für einfache, fortgeschrittene und qualifizierte Signaturen ausgestellt wurden. Insbesondere gilt sie für die Erbringung aller unter ⇨1.6 Definitionen und Kurzbezeichnungen / Definitions and acronyms (p16) definierten Zertifizierungsdienste.

Zeitstempeldienste, serverseitige oder mobile Signaturdienste können als qualifizierte, fortgeschrittene oder einfache elektronische Signaturdienste angeboten werden. Mobile Signaturdienste werden mittels Mobiltelefone oder anderer mobiler technischer Einheiten ausgelöst. Mobile Signaturdienste werden als Serverdienste oder als "direkte elektronische Signatur" (Signatur am Endgerät) in der mobilen technischen Einheit angeboten.

Die ausgestellten einfachen Zertifikate können vom Signator sowohl zur Durchführung von Geheimhaltungsoperationen (Verschlüsselung), als auch zum Signieren einzelner oder mehrerer elektronischer Dokumente verwendet werden.

Die ausgestellten qualifizierten Zertifikate dienen zum Signieren (elektronische Signatur oder qualifizierte elektronische Signatur) einzelner oder mehrerer elektronischer Dokumente (Dateien).

9.16 Sonstige Bestimmungen / Miscellaneous provisions

9.16.1 Vollständigkeitserklärung / Entire agreement

Gemäß GLOBALTRUST® Certificate Policy

9.16.2 Abgrenzungen / Assignment

Gemäß GLOBALTRUST® Certificate Policy

9.16.3 Salvatorische Klausel / Severability

Gemäß GLOBALTRUST® Certificate Policy

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) / Enforcement (attorneys' fees and waiver of rights)

Der Zertifizierungsbetrieb auf Basis dieser GLOBALTRUST® Certificate Practice Statement wird erst nach Genehmigung durch die zuständigen Aufsichtsstellen vorgenommen.

9.16.5 Höhere Gewalt / Force Majeure

Gemäß GLOBALTRUST® Certificate Policy

9.17 Andere Bestimmungen / Other provisions

Gemäß GLOBALTRUST® Certificate Policy

VERZEICHNISSE

Autor(en) und Gültigkeitshistorie

Die historischen Versionen dieses Dokuments sind über die Website des Betreibers abrufbar.

Die Gültigkeit der jeweiligen Dokumente ergibt sich aus dem Beginndatum der Gültigkeit und dem Beginndatum der Gültigkeit des nächstfolgenden Dokuments. Sofern nicht anders vermerkt endet die Gültigkeit des alten Dokuments am Vortag der Gültigkeit des neuen Dokuments.

Name	Version	Stand	Datei	Kommentar
Hans G. Zeger	Version 1.0	1. Juni 2014		Stammfassung
Hans G. Zeger	Version 1.0a	1. Februar 2015	globaltrust-certificate-practice.pdf	Ergänzungen zum Zeitstempeldienst

ANHANG

ANHANG A: DOKUMENTATION

1 BIBLIOGRAPHIE

⇨ GLOBALTRUST® Certificate Policy Anhang A: 1 Bibliographie